UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,184	09/25/2003	Eduard K. de Jong	SUN-040027	9837

24209 7590 06/13/2007

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
06/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,184	DE JONG, EDUARD K.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *5,10,15 and 20* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-9,11-14 and 16-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/03 and 5/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Applicant's election with traverse of group I (claims 1-4, 6-9, 11-14, and 16-19) in the reply filed on 3/26/2007 is acknowledged. The traversal is on the ground(s) that the MPEP draws distinctions between subcombinations and processes of making and using and delineates different requirements that the examiner must show in each case and that the examiner's characterization of the groups as subcombinations is incorrect and that a showing that the process of making and the process of using are independent and distinct has not been made. This argument is not found persuasive because the MPEP does not draw a distinction between subcombinations and process of making and using. The MPEP sets forth guidelines on subcombinations. It sets forth guidelines on product and process of making. It sets forth guidelines on product and process of using. It also sets forth guidelines on product, process of making and process of using. However, there is no guideline on just process of making and using. Where there are claims which only defines process of making and using, the examiner respectfully submits that the best way to characterize the claims is as subcombinations disclosed as usable together. A search for a process of making a product does not necessarily encompass a search for a process of using the product and vice versa. Because the groups were properly characterized and there would burden on the examiner to search two independent and distinct inventions, the restriction requirement as set forth in the prior office action was correct.

The requirement is still deemed proper and is therefore made FINAL. Claims 5, 10, 15, and 20 are withdrawn from consideration. Claims 1-4, 6-9, 11-14, and 16-19 were examined.

Information Disclosure Statement

The references listed in the IDS's submitted on 12/15/2003 and 5/7/2007 were considered.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 11-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 11-14 are directed towards an apparatus comprising various means for application program obfuscation. While the claims appear to invoke 112, 6th paragraph via use of means plus function language, the specification failed to describe the structure of the claimed means. As such, it is assumed that the claims were not meant to invoke 112, 6th paragraph and in interpreting the claims in a broad, yet reasonable manner, it is submitted that the various means recited in the claims could have been implemented in software alone. As such, claims 11-14 are rejected as being non-statutory since the claims are directed towards software per se.

Claims 16-19 are directed towards an apparatus for application program obfuscation comprising an application program provider. The claimed application program provider appears to be implemented via software alone, thus claims 16-19 are not statutory due to being directed towards software per se.

The above 101 rejections can be overcome by reciting at least one component as part of the claimed apparatus that has hardware.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4, 6-7, 9, 11-12, 14, 16-17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al (US 7,170,999) in view of Okada (US 6,789,177) in further view of LeVine et al (US 2002/0120854) and in further view of applicant submitted document to Collberg et al ("A Taxonomy of Obfuscating Transformations", published in 1997).

Claims 1, 6, 11, and 16:

As per claim 1, Kessler discloses "receiving a reference to a decryption algorithm and a first cryptographic key and creating a key decryption program comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key" (col 8, lines 50-67 and col 10, lines 58-67). *Note that transfer key TK was encrypted using PK2. The cited portion of Kessler*

discloses use of decryption software which uses SK2, i.e. said first cryptographic key, to extract TKI. The recited limitations reads on receiving the source code to a decryption algorithm and compiling the source code to create a key decryption program which makes use of a first cryptographic key in the decryption process. Since the client software is able to decrypt the encrypted key TK, source code must have been received and compiled to create the client software disclosed by Kessler.

Kessler further discloses applying a cryptographic process to a second cryptographic key together with a public cryptographic key to create an encrypted second cryptographic key (col 5, lines 29-42). *Track key TK is considered the second cryptographic key.*

Kessler discloses sending said key decryption program, i.e. client software (col 4, lines 44-46). *The cited portion discusses clients receiving the client software, thus the client software was sent.*

The difference between Kessler's disclosed invention and applicant's claimed invention is that Kessler uses a public key PK2 to encrypt the second cryptographic key, i.e. track key TK, and decrypts TK using a secret key SK2. From the way applicant's claimed invention is recited, it appears that the second key is both encrypted and decrypted using a first cryptographic key, i.e. via a symmetric encryption scheme. Kessler also does not explicitly disclose "scrambling said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key description program, said obfuscation descriptor based at least in part on a target ID."

As such, whereas Kessler merely sends a key decryption program, applicant's claimed invention sends an obfuscated key decryption program.

However, Okada discloses using a first cryptographic key, i.e. session key, for both encrypting and decrypting a second key, i.e. content key (col 9, lines 21-26 and col 10, lines 39-53). In light of this teaching by Okada, at the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Kessler's invention such that instead of using an asymmetric key system to encrypt and decrypt the second cryptographic key, a symmetric key system was used instead such that a first cryptographic key was used to both encrypt and decrypt the second cryptographic key disclosed by Kessler. One skilled would have been motivated to do so because symmetric key systems are faster and less computationally intensive than asymmetric key systems.

Further, LeVine discloses scrambling an encrypted second cryptographic key into an instruction stream of a program using a code obfuscation method, said scrambling creating an obfuscated program (Fig 8, item 45 and paragraphs 21 and 23). Collberg discloses the obfuscation method used for obfuscation being indicated by an obfuscation descriptor, said obfuscation descriptor based at least in part on a target ID (p3, second column, first paragraph and p4, first column, first paragraph).

In light of the above further teachings, it would have been obvious to one of ordinary skill in the art to further modify Kessler's invention according to the limitations recited in claim 1 by using the encrypted second cryptographic key in an obfuscation method to generate an obfuscated key description program and sending the obfuscated

key decryption program. One skilled would have been motivated to obfuscate the key decryption program of Kessler as per LeVine's teachings because obfuscating the decryption software would make debugging and cracking the software by an unauthorized party a nontrivial task (LeVine: paragraph 14). Note that this would make the content accessed by the decryption software more secure also. One skilled would have incorporated Collberg's teachings of an obfuscation descriptor because it would allow the receiver of the client software taught by Kessler to choose the level of obfuscation that his/her architecture and operating system is capable of handling.

Claims 6, 11, and 16 recite limitations substantially similar to what is recited in claim 1 and are rejected for substantially similar reasons.

Claims 2, 7, 12, and 17:

Kessler further discloses method, medium, means, and apparatus for sending digital content protected by said second cryptographic key (Fig 2 and col 10, lines 58-67).

Claims 4, 9, 14, and 19:

Collberg discloses wherein said target ID comprises a VM ID (p3, last paragraph of column 1-first paragraph of column 2). Note that when downloading software, i.e. the client software disclosed by Kessler, Collberg discloses that the architecture of the user would have to be identified. This would include the Java VM ID since obfuscation as per Collberg's invention is accomplished in Java. Such information is needed to ensure proper functionality of the decryption program.

Claims 3, 8, 13, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al (US 7,170,999) in view of Okada (US 6,789,177) in further view of LeVine et al (US 2002/0120854) and in further view of applicant submitted document to Collberg et al ("A Taxonomy of Obfuscating Transformations", published in 1997) and further in view of Shinn Orr et al (WO 02/079955), herein referred to as Shinn and which was also submitted by applicant.

Claims 3, 8, 13, and 18:

Kessler does not explicitly disclose method, medium, means, and apparatus for sending said obfuscated key decryption program together with said digital content. However, the limitation is disclosed by Shinn (p19, line 32-p20, line 8).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Kessler's invention according to the limitations recited in claims 3, 8, 13, and 18. One skilled would have been motivated to send said obfuscated decryption program together with said digital content because Shinn discloses that in doing so, attacks by reverse-engineering may be delayed until the last possible moment before the program is used (p20, lines 5-8).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100